WEBINAR EVENT:

ENTERPRISE-WIDE KUBERNETES

Episode 2: Security

October 18, 2018, at 11 am PT / 2 pm ET

nirmata

Jim Bugwadia
CEO

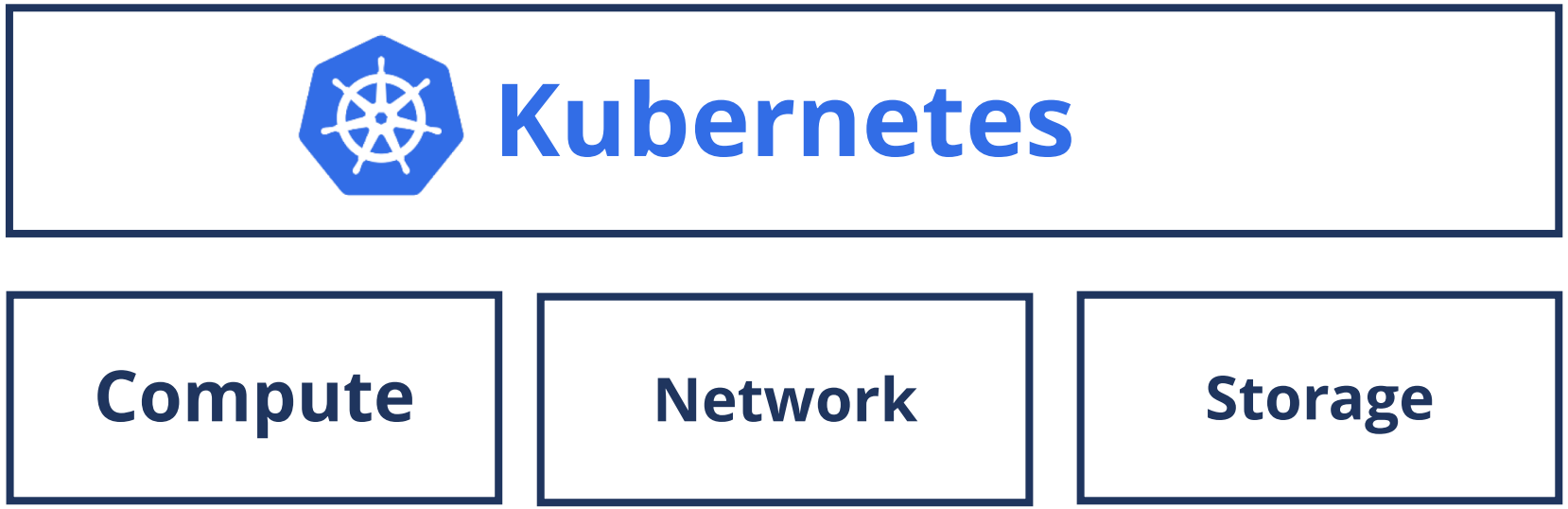
Twistlock

Patrick Maddox
Senior Director,
Solution Architecture

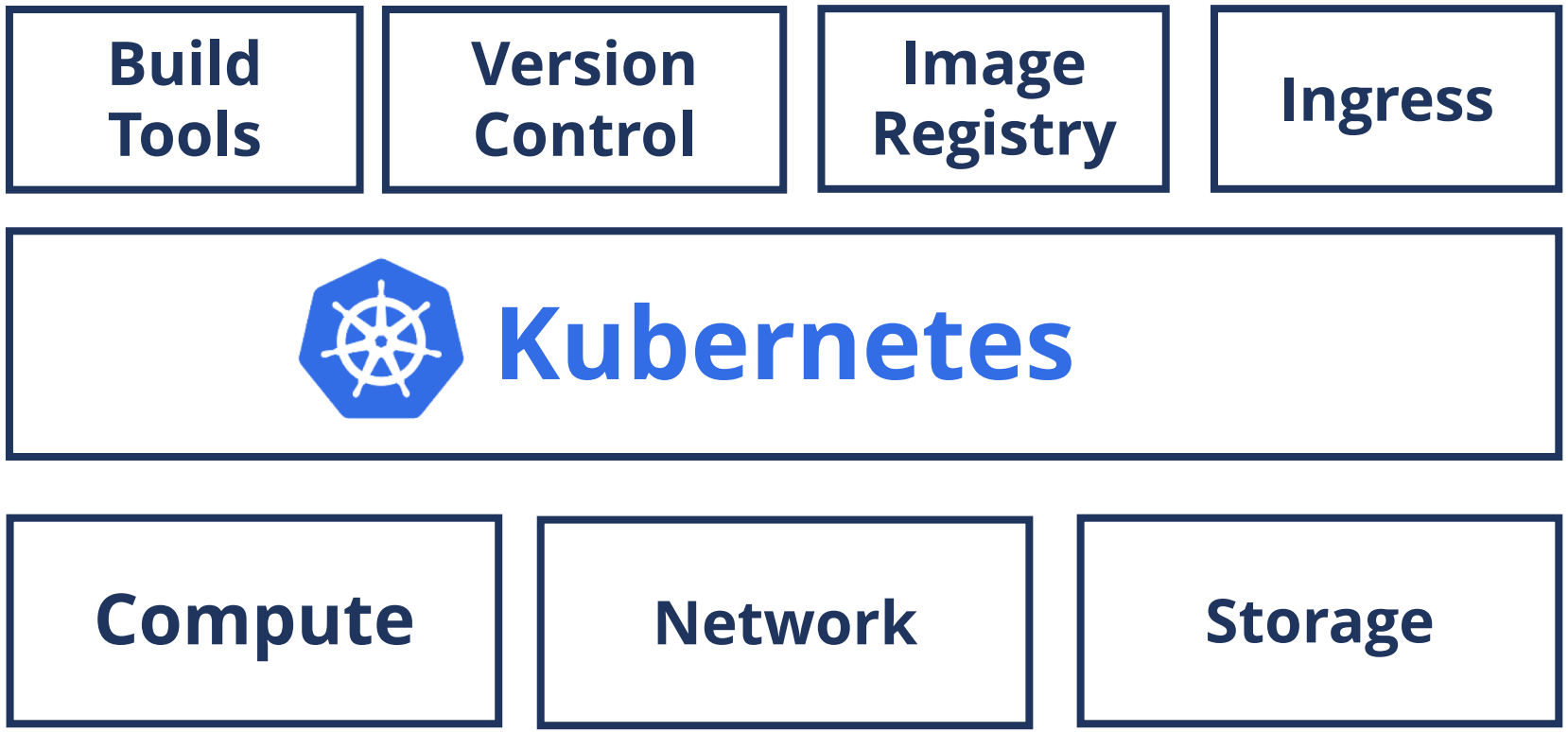
Kubernetes is the Multi-Cloud OS for Enterprises

- Production-grade container orchestration
- Works on any cloud
- Large ecosystem

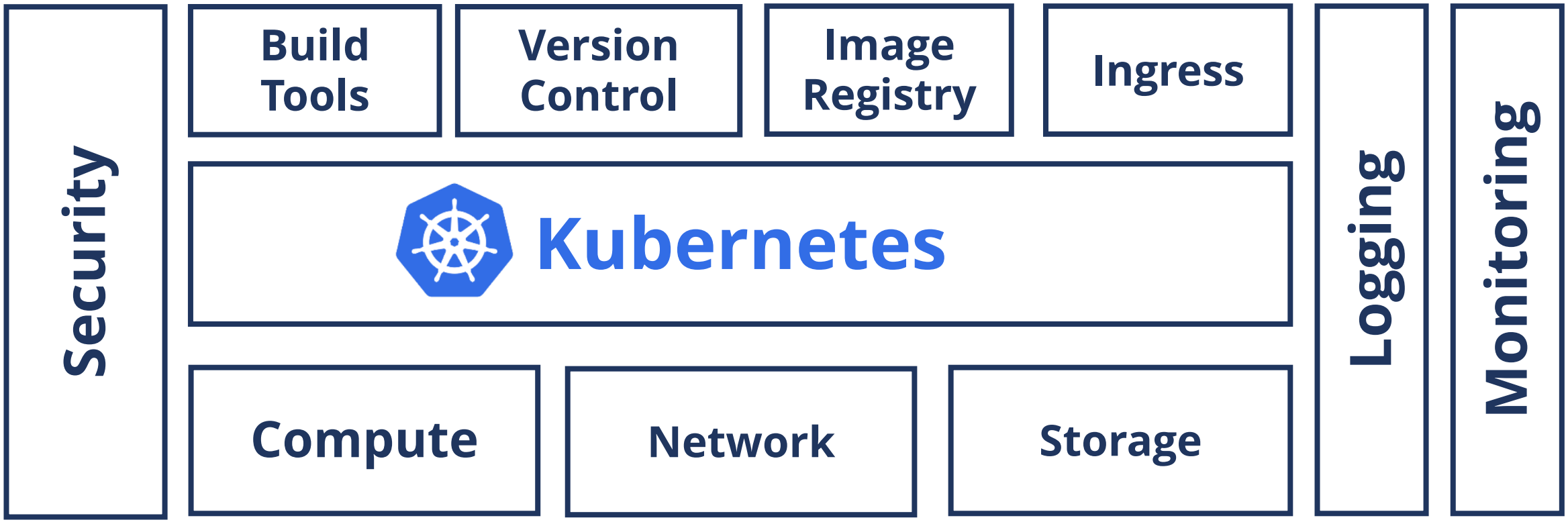
The Enterprise-wide Kubernetes Stack



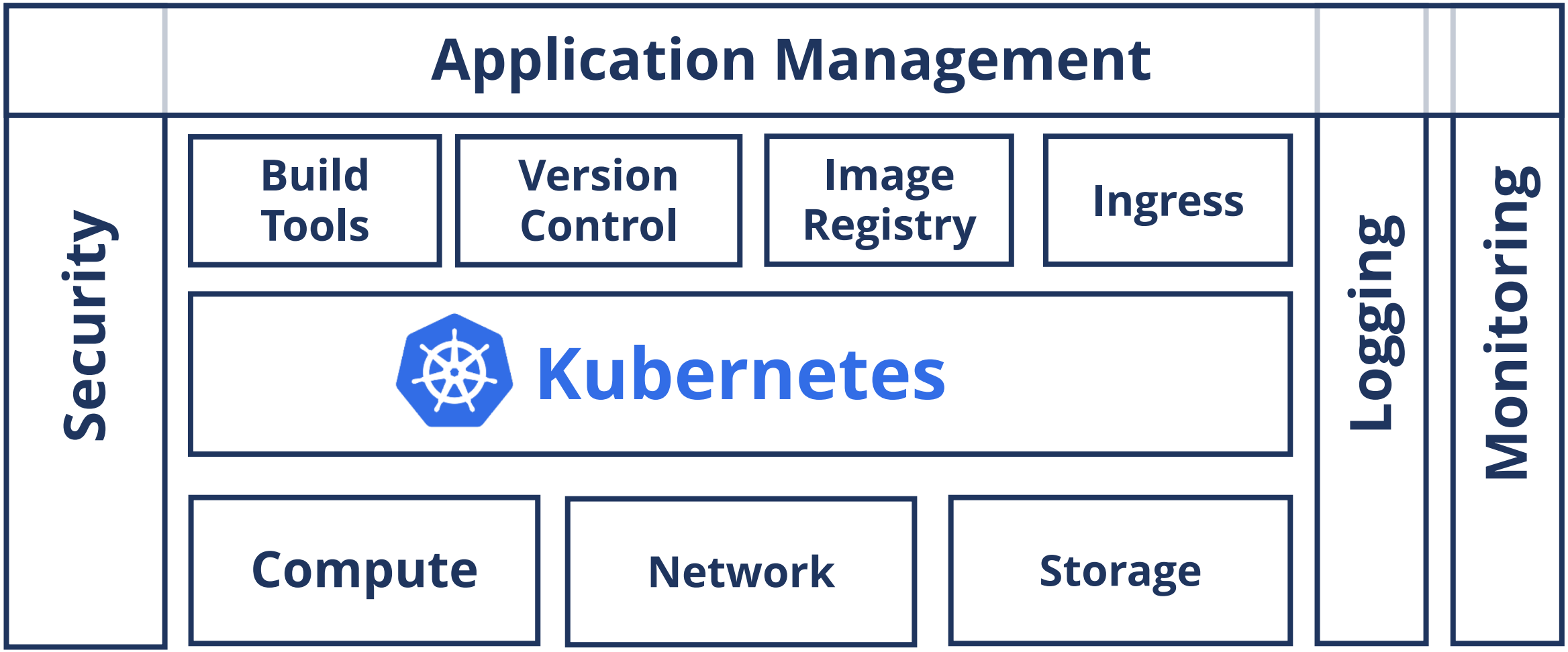
The Enterprise-wide Kubernetes Stack



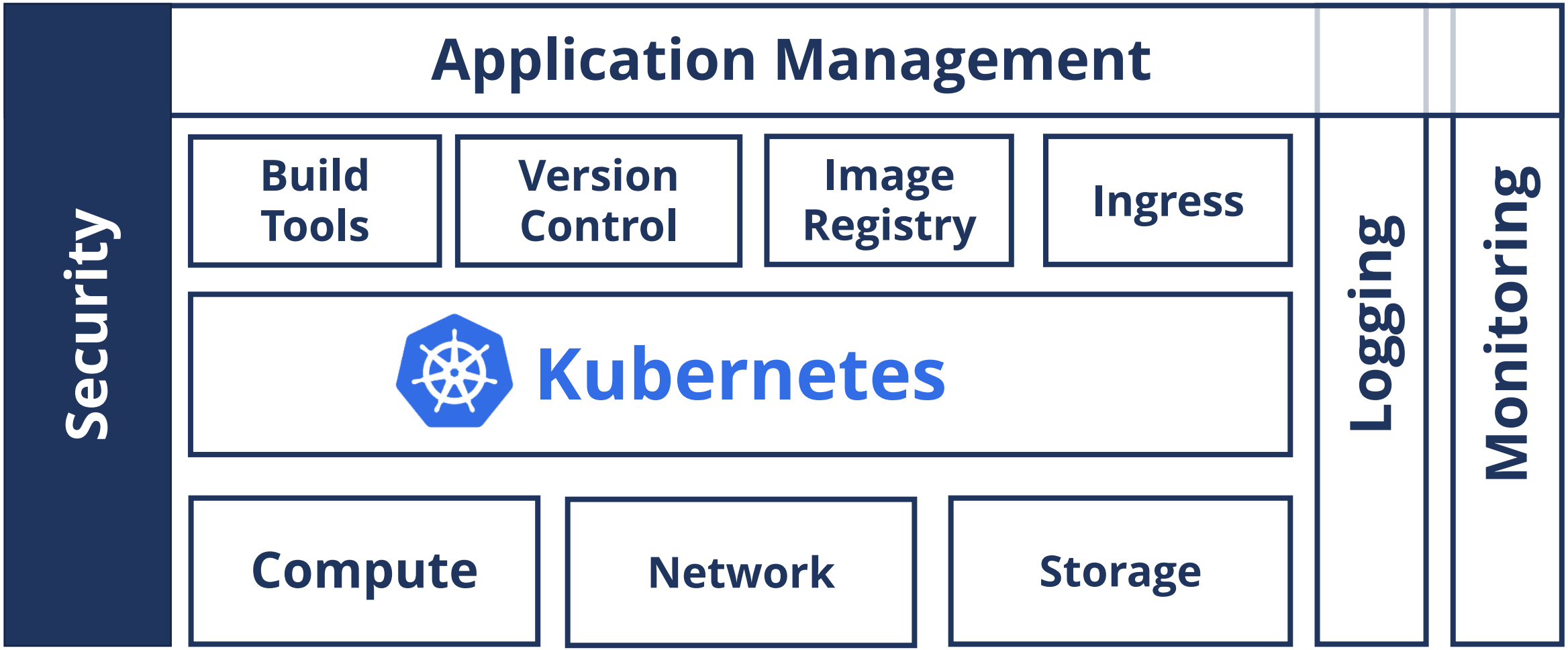
The Enterprise-wide Kubernetes Stack



The Enterprise-wide Kubernetes Stack



The Enterprise-wide Kubernetes Stack



Patrick Maddox

- Senior Director, Solutions Architecture @ Twistlock
- Previously led Solutions Engineering and Services at Puppet
- Multiple roles from architecture to operations at Verizon

Kubernetes Security

What are the top things I need to do to secure my cluster?

What do I need to consider for securing applications deployed in the Kubernetes cluster?

How do I evaluate and compare the security solutions in the CNCF ecosystem?

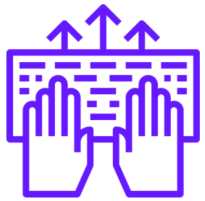
Twistlock™

Twistlock

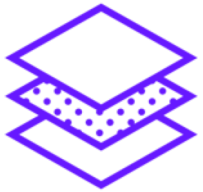
Basic Security for Deployment

Patrick Maddox
Director – Sol. Architecture, Twistlock

What is Twistlock?



IN THE BUILD



AT THE REGISTRY

IN PRODUCTION

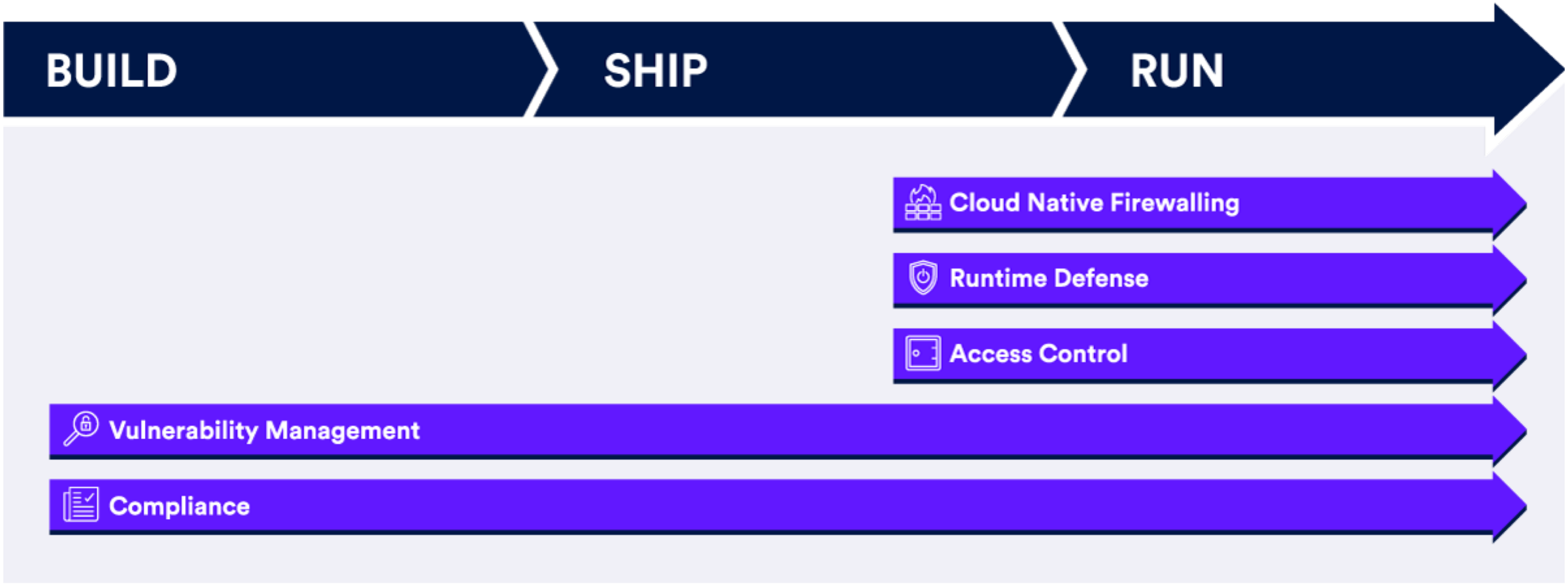
Cloud native cybersecurity

from beginning to end of the lifecycle

Cloud native cybersecurity

from top to bottom of the stack

Security for the entire Container Lifecycle



Securing the Stack

- Secure the Hosts
- Secure Kubernetes
- Implement Kubernetes RBAC
- Evaluate against the Linux, Docker, Kubernetes CIS Benchmarks
- Secure the Workloads

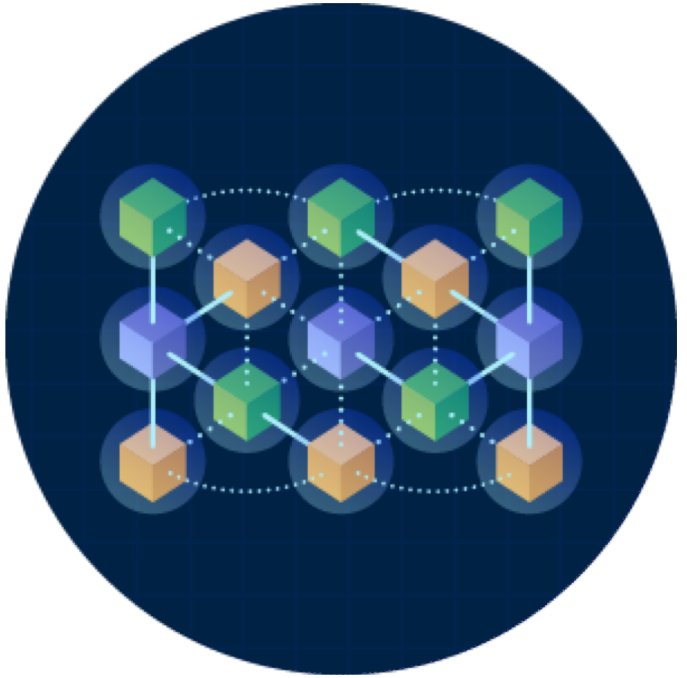
TWISTLOCK | © 2018 | Confidential

Secure the host

- Minimal install of the OS
- Update your packages
- Remove unneeded services
- Close any open ports you don’t need
- Secure login by certificates
- Intrusion detection systems

Secure Kubernetes

- RBAC
- Layer 3 Protection
- Configure the Master Nodes
- Configure the Worker Nodes
- ETCD
- Secrets Injection



Kubernetes RBAC

- White list security model that is additive
- Role / RoleBinding
- ClusterRole / ClusterRole Binding
- Limit access to your nodes
- Access to containers in the cluster should be done through kubectl

Linux, Docker, and Kubernetes CIS Benchmarks

- Apply to the Hosts
- Apply to the Docker Engine
- Apply to the Master Nodes
- Apply to the Worker Nodes

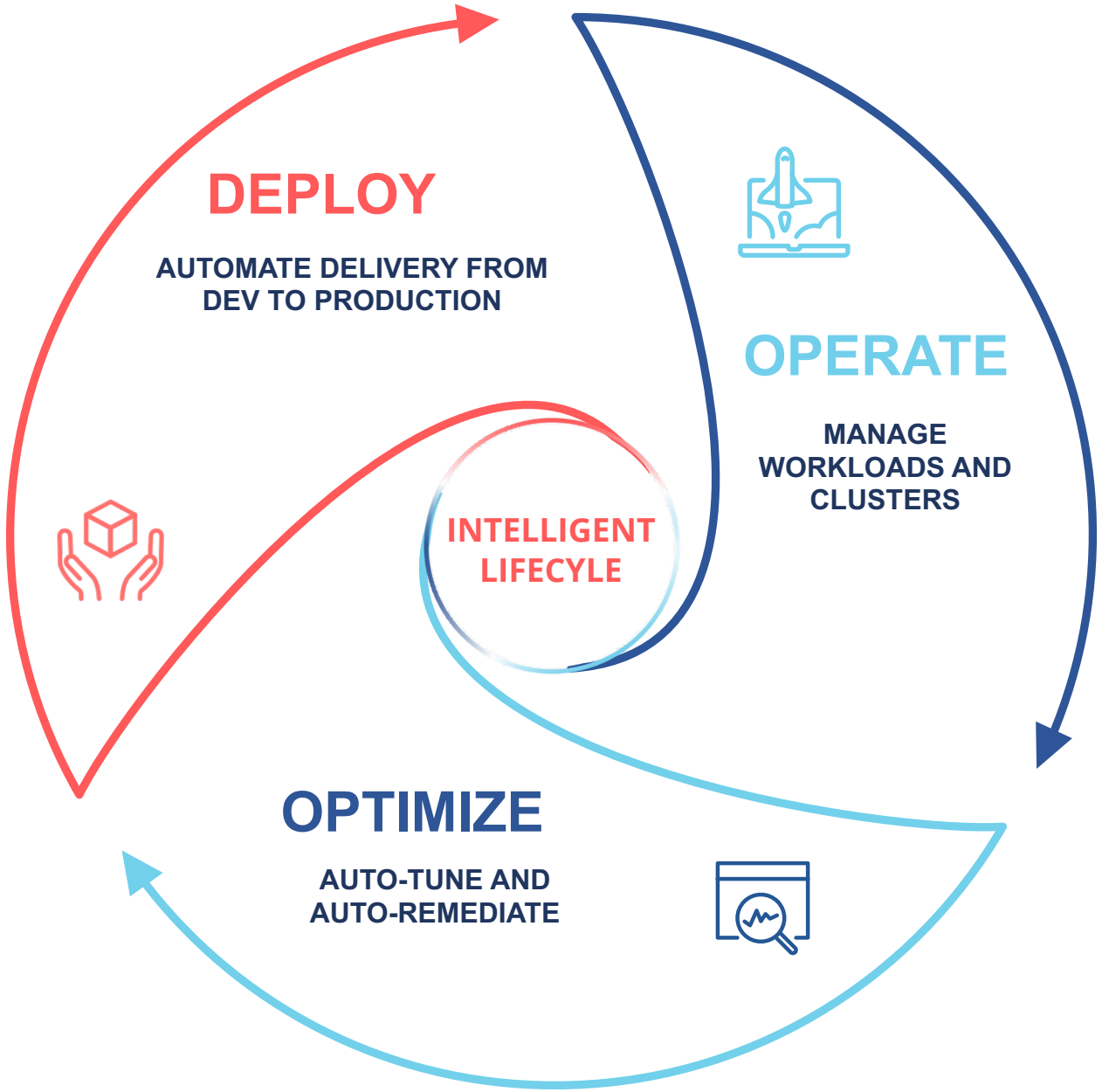
Secure the Network and Workloads

- Automatically segment your infrastructure
- Automatically model your applications and their behaviors
- Eliminate manual policy creation and maintenance wherever possible

Demo!

Nirmata

Nirmata


DEPLOY
AUTOMATE DELIVERY FROM DEV TO PRODUCTION
OPERATE
MANAGE WORKLOADS AND CLUSTERS
INTELLIGENT LIFECYLE
OPTIMIZE
AUTO-TUNE AND AUTO-REMEDIATE

Nirmata Architecture

Any Application. Any OS. Any Infrastructure.

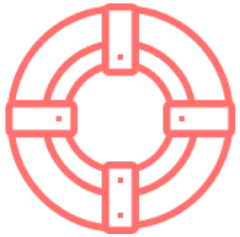
Nirmata Features

Composable

Design your own Kubernetes stack.
Nirmata ensures consistency.

Enterprise Grade

Single pane of glass management across clusters. Metrics, alarms, remediation.



100% Upstream

Any Kubernetes distribution, release.
Eliminate curation and lock-in.

As a Service or On-Prem

Your choice. Based on your company privacy and compliance regulations.

Cloud Flexible

Public, private, hybrid, or bare-metal.
Install new, or manage existing, clusters.

White Glove Service

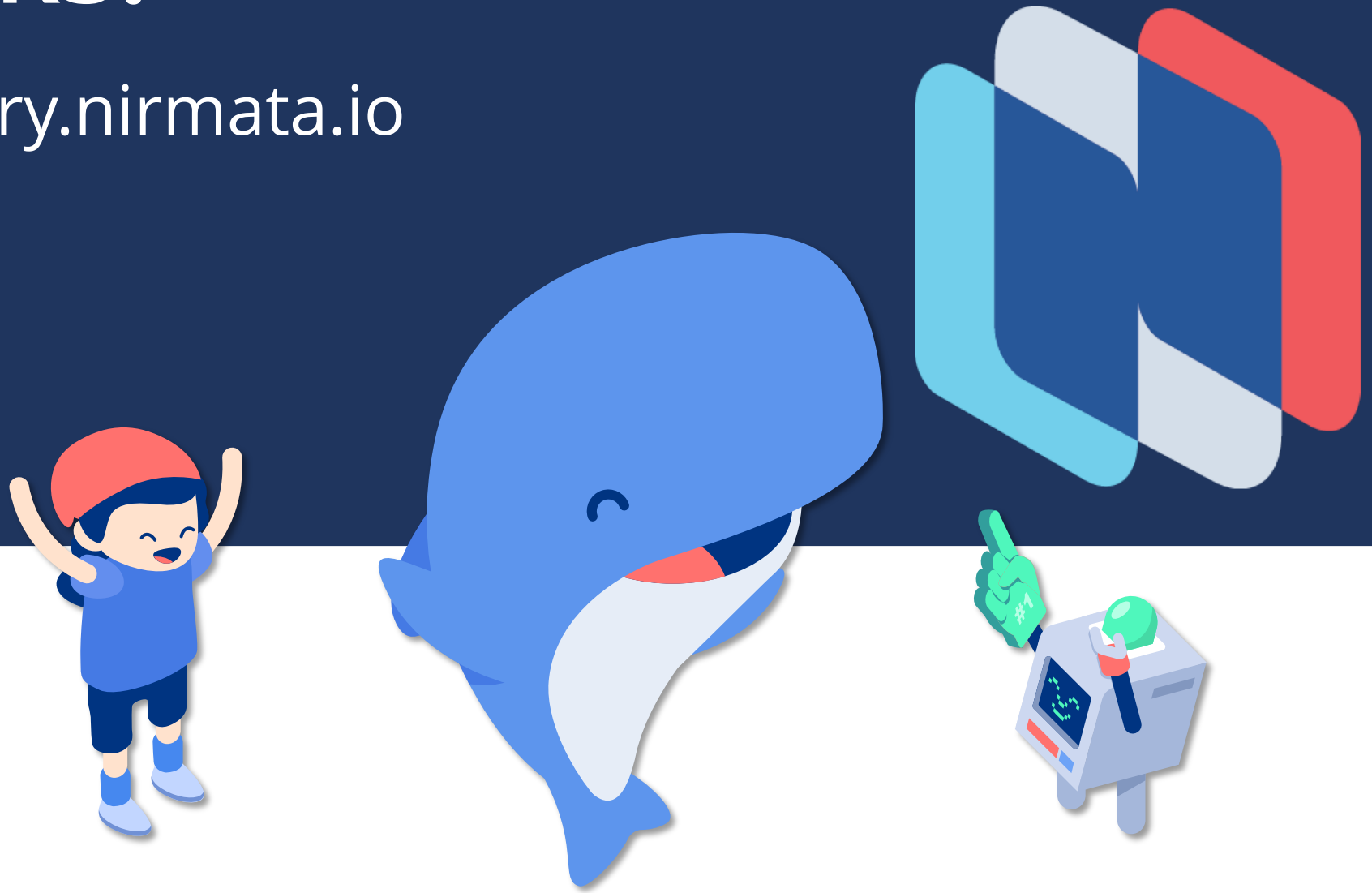
Experienced enablement team supports you at every step of your journey.

Demo

Summary

- ☑ A complete Kubernetes security strategy spans hosts, clusters, containers, and applications across build and runtime environments.
- ☑ Twistlock provides a comprehensive Kubernetes security solution
- ☑ Nirmata enables consistency and compliance across Kubernetes clusters

Q & A

Thanks!

https://try.nirmata.io